AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

VINCENT GLYNN BENNETT JR.,

Defendant(s)

Case No. 2:23-mj-01972

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of April 21, 2023, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1), (b)(1)(A)(ii)	Possession with Intent to Distribute a Controlled Substance

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/ Austin Koval
Complainant's signature

Austin Koval, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: April 22, 2023

Alicia G. Rosenberg
Judge's signature

City and state: Los Angeles, California

Hon. Alicia G. Rosenberg, U.S. Magistrate Judge
Printed name and title

AUSA: Alix McKenna

AFFIDAVIT

I, Austin Koval, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against VINCENT GLYNN BENNETT JR. ("BENNETT") for a violation of 21 U.S.C. § 841(a)(1): Possession with Intent to Distribute a Controlled Substance. This affidavit is also made in support of a search warrant for a green iPhone in a black case currently in the custody of HSI, in Los Angeles, California (the "SUBJECT DEVICE"), as described more fully in Attachment A.

2. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

3. The facts set forth in this affidavit are based upon my personal observations; my training and experience; and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and part only.

II. BACKGROUND OF AFFIANT

4. I am a Special Agent ("SA") with the Department of Homeland Security ("DHS"), Homeland Security Investigations ("HSI") and I have been so employed since 2019. As an HSI SA, I received training at the Federal Law Enforcement Training Center ("FLETC") that included courses on conducting criminal investigations, narcotics identification, narcotics trafficking, organized crime, gangs, drug trafficking organizations, firearms trafficking, human trafficking, murder investigations, processing of crime scenes, collection of evidence, and other law enforcement topics. Prior to HSI, I was employed as a Special Investigator with the State of Arizona Office of Inspector General Criminal Investigations Unit. I have conducted multiple complex criminal investigations for multiple violations of federal and state laws including, but not limited to criminal conspiracy, organized crime, fraud, forgery, crimes against children, firearms, narcotics, money laundering, embezzlement, trafficking, identity theft, public corruption, and financial crimes. I further served as a Field Training Officer ("FTO") for newly hired investigators, and I am cross trained as a forensic interviewer. I graduated Summa Cum Laude from Arizona State University in 2016 with a bachelor's degree in Criminology and Criminal Justice and have completed numerous advance trainings in criminal investigations, organization crime, narcotics, gangs, murder investigations, and human trafficking. I have become familiar with the methods, language, structures, and criminal activities of drug trafficking

organizations operating within and outside of this judicial district. I have investigated drug trafficking occurring through airports and I am familiar with the methods used to traffic illegal narcotics through airports including the concealment methods used. I am familiar with the way narcotics are wrapped and transported by those attempting to transport illegal narcotics.

5. As an HSI SA, I have conducted criminal investigations involving narcotics trafficking, gangs, organized crime, racketeering, firearms trafficking, gang murders, human trafficking, criminal conspiracy, money laundering, child exploitation, immigration fraud, trade fraud, violations of the Protect Act, illegal exports, and intellectual property crimes. I have participated in the execution of search and arrest warrants and seized evidence of federal and state law as the case agent and in a secondary role.

III. SUMMARY OF PROBABLE CAUSE

6. On or about April 21, 2023, Transportation Security Administration ("TSA") officers at Hollywood Burbank Airport in Burbank, California, discovered a piece of carry-on luggage belonging to BENNETT that contained four sealed packages of suspected narcotics. Each of the four packages weighed approximately five pounds, for a combined weight of approximately twenty pounds. Special Agent Masood Azaran conducted a field test of the suspected narcotics, which tested presumptively positive for cocaine. During a Mirandized interview, BENNETT stated that he had previously flown to

California, he had the packages because he was "just money hungry," and he expected to make anywhere from $20,000 to $100,000. Law enforcement arrested BENNETT, who possessed the SUBJECT DEVICE on his person.

IV. STATEMENT OF PROBABLE CAUSE

7. Based on my personal involvement, and my conversations with TSA officers, Burbank-Glendale-Pasadena Airport Authority Police Department ("BGPAPD") officers, witnesses, and other HSI SAs, I know the following:

A. SUSPECTED DRUGS FOUND IN BENNETT'S BAGGAGE

8. On April 21, 2022, at approximately 9:05 a.m., TSA Officer Isaac Ramirez was operating a bag check x-ray machine to screen luggage at Hollywood Burbank Airport in Los Angeles County for passengers leaving on domestic flights. BENNETT placed a medium sized grey suitcase ("the suspect bag") on the x-ray machine. The TSA security screening area was equipped with surveillance cameras. I reviewed footage and saw BENNETT place the suspect bag on the belt leading to the X-ray machine.

9. Officer Ramirez noticed a mass inside the suspect bag, which was not uniform and had cracks. Based on his training and experience, including the recognition of narcotics on x-ray machines, the mass appeared to be consistent with illegal narcotics. The suspect bag was opened, and TSA officers discovered four items or bundles tightly wrapped in plastic and tape.

10. TSA Officer Greg Heine, a supervisor, asked BENNETT what the four bundles contained. BENNETT initially indicated

that the bundles contained books, then changed his response and stated that they contained food and snacks.

11. The bundles were subsequently provided to BGPAPD Officer Quesada for further investigation. Officer Quesada asked BENNETT if the suspect bag and its contents belonged to him, and BENNETT confirmed that they did. Officer Quesada asked what was in the four wrapped bundles. BENNETT responded that it was food. BENNETT offered to open to suspect packages and stated that they were "just edibles." Based on my training and experience, I know that "edibles" is a common term for marijuana-infused food items. Later during the conversation, BENNETT stated that he didn't know what they contained.

12. TSA officers opened one of the bundles and discovered a white powdery substance inside, resembling cocaine. TSA officers conducted an explosive trace detection test on the substance, but the results came back negative for explosives.

13. BGPAPD Officers took custody of the bag, and Special Agents ("SA") from Homeland Security Investigations ("HSI") arrived to assist with the investigation. Special Agents inspected the four bundles. One had previously been opened by a TSA officer, and each bundle contained two brick-like shapes. Each bundle had written markings on it. Based on my training and experience, the packaging and markings were consistent with packaging commonly used by members of drug trafficking organizations. In my experience it is common for members of drug trafficking organization to mark their product with letters or numbers as an identifier.

14. I observed a white powdery substance inside the bundle that had been opened. Based on my training and experience, the white powdery substance was consistent in appearance with powder cocaine. SA Masood Azaran also conducted a test for drugs on a portion of the suspected cocaine using TruNarc, a hand-held narcotics analyzer, which tested presumptively positive for cocaine.

B. INTERVIEW OF BENNETT

15. On April 21, 2022, at approximately 3 p.m., I read BENNETT his Miranda rights out loud in English. BENNETT acknowledged he fully understood the information read to him regarding the statement of rights and signed a waiver of rights form. BENNETT agreed to speak with me and my partner, SA Azaran.

16. BENNETT initially told us that he came to Los Angeles for a vacation. However, when I asked him to explain why he had the items in his suitcase, he responded by saying he was "just money hungry". BENNETT stated that he expected to make anywhere from $20,000 to $100,000, though he also claimed that he never opened the suitcase and didn't know what was inside.

17. Prior to the interview, I observed surveillance footage in which BENNETT appeared to be on the phone while TSA officers were inspecting his bag. I asked him about this phone exchange. BENNETT told me that he had called his cousin and told him that he got caught.

18. BGPAPD officers obtained custody of BENNETT'S cellular phone, a green iPhone in a black case (i.e., the SUBJECT DEVICE) from BENNETT's person.

V. TRAINING AND EXPERIENCE ON DRUG OFFENSES

19. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where the drug trafficker has ready access to them, such as on their cell phones and other digital devices.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of the drugs between the seller and the buyer, the negotiation of price, and discussion

of whether or not participants will bring weapons to a deal. In addition, it is common for people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices, including in the form of calendar entries and location data.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES

20. As used herein, the term "digital device" includes the SUBJECT DEVICE.

21. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary

directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously

develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

22. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it can take a substantial period of time to search a digital device for many reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

23. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To

unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. The person who is in possession of a device or has the device among his or her belongings is likely a user of the device. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress BENNETT's thumb and/or fingers on the device; and (2) hold the device in front of BENNETT's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

24. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

25. Based on the foregoing facts and opinions, and on my training and experience, I believe that there is probable cause to believe that BENNETT violated Title 21, United States Code, Section 841(a)(1): Possession with Intent to Distribute a Controlled Substance. There is also probable cause that the items to be seized described in Attachment B will be found in a search of the SUBJECT DEVICE described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 22nd day of April, 2023.

Alicia G. Rosenberg

THE HONORABLE ALICIA G. ROSENBERG
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

PROPERTY TO BE SEARCHED

The following digital device (the "SUBJECT DEVICE"), seized on April 21, 2023, and currently maintained in the custody of the Department of Homeland Security in Los Angeles, CA: a green iPhone device in a black case, discovered on the person of VINCENT GLYNN BENNETT JR. ("BENNETT").

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances) and 21 U.S.C. § 846 (conspiracy and attempt to distribute controlled substances) (the "Subject Offense"), namely:

a. Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

b. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violation;

c. Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show instant and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violation;

d. Records, documents, programs, applications, materials, or conversations relating to the trafficking of drugs, including ledgers, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed;

e. Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

f. Contents of any calendar or date book;

g. Global Positioning System ("GPS") coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

a. Any SUBJECT DEVICE which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offenses, and forensic copies thereof.

b. With respect to any SUBJECT DEVICE containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. applications, programs, software, documentation, manuals, passwords, keys, and other access devices that may be necessary to access the device or data stored on the device, to run software contained on the device, or to conduct a forensic examination of the device;

vii. records of or information about Internet Protocol addresses used by the device.

2. As used herein, the terms "records," "information," "documents," "programs," "applications," and "materials" include records, information, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

II. SEARCH PROCEDURE FOR THE SUBJECT DEVICE

3. In searching the SUBJECT DEVICE (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") may search any SUBJECT DEVICE capable of being used to facilitate the above-listed violations or containing data falling within the scope of the items to be seized.

b. The search team will, in its discretion, either search each SUBJECT DEVICE where it is currently located or transport it to an appropriate law enforcement laboratory or similar facility to be searched at that location.

c. The search team shall complete the search of the SUBJECT DEVICE as soon as is practicable but not to exceed 120 days from the date of issuance of the warrant. The government will not search the digital device(s) and/or forensic images thereof beyond this 120-day period without obtaining an extension of time order from the Court.

d. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each SUBJECT DEVICE capable of containing any of the items to be seized to the search protocols to determine whether the SUBJECT DEVICE and any data thereon falls within the scope of the items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the scope of the items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase," "Griffeye," and "FTK"

(Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

e. The search team will not seize contraband or evidence relating to other crimes outside the scope of the items to be seized without first obtaining a further warrant to search for and seize such contraband or evidence.

f. If the search determines that a SUBJECT DEVICE does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the SUBJECT DEVICE and delete or destroy all forensic copies thereof.

g. If the search determines that a SUBJECT DEVICE does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

h. If the search determines that the SUBJECT DEVICE is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

i. The government may also retain a SUBJECT DEVICE if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been

able to fully search a device because the device or files contained therein is/are encrypted.

j. After the completion of the search of the SUBJECT DEVICE, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

4. The review of the electronic data obtained pursuant to this warrant may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the investigating agency may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

5. During the execution of this search warrant, law enforcement is permitted to (1) depress BENNETT's thumb- and/or fingers onto the fingerprint sensor of the SUBJECT DEVICE (only if the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of BENNETT's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more

than objectively reasonable force in light of the facts and circumstances confronting them.

6. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.